AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method of encryption of data in a digital television system communicated between a first decoder and a portable security module ~~second device~~, wherein at least one precalculated key pair is stored in a memory of the first decoder ~~device~~, said at least one key pair comprising a session key and an encrypted version of the session key prepared using a transport key, the encrypted version of the session key being subsequently communicated to the portable security module ~~second device~~ which decrypts the encrypted version using an equivalent transport key stored in its memory such that data communicated from at least the ~~second~~ portable security module to the first decoder ~~device~~ may thereafter be encrypted and decrypted by the session key ~~in the respective devices~~.

2. (Currently Amended) A method as claimed in claim 1, in which a plurality of key pairs are stored in the memory of the first decoder ~~device~~, the first decoder ~~device~~ selecting and processing at least one session key to generate a definitive session key and communicating the associated encrypted version of said at least one session key to the ~~second device~~ portable security module for decryption and processing by the ~~second device~~ portable security module to generate the definitive session key.

3. (Currently Amended) A method as claimed in claim 2 in which a subset of a plurality of stored session keys is chosen by the first decoder ~~device~~ to generate the definitive session key, the associated encrypted versions of the subset of session keys being communicated to the ~~second device~~ portable security module for decryption and processing.

4. (Currently Amended) A method as claimed in claim 2 ~~or 3~~, in which the order of

combination of a plurality of session keys used to generate the definitive session key is communicated from the first decoder to the ~~second device~~ portable security module.

5. (Currently Amended) A method as claimed in claim 4 in which an initial session key value known to both the first decoder and the ~~second device~~ portable security module is repeatedly encrypted in both devices by an ordered sequence of session keys using an encryption algorithm sensitive to the order of encryption.

6. (Currently Amended) A method as claimed in ~~any preceding~~ claim 1 in which said at least one precalculated key pair is selected from a larger set of precalculated key pairs prior to being stored in the first decoder ~~device~~.

7. (Currently Amended) A method as claimed in ~~any preceding~~ claim 1 in which the encrypted version of a session key communicated to the ~~second device~~ portable security module also includes a signature value readable by the ~~second device~~ portable security module to verify the authenticity of the encrypted version of the session key.

8. (Currently Amended) A method as claimed in ~~any preceding~~ claim 1 in which an algorithm and transport key used to encrypt and decrypt a session key correspond to a symmetric algorithm and associated symmetric key.

9. (Currently Amended) A method as claimed in ~~any preceding~~ claim 1 in which an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the ~~second device~~ portable security module corresponds to a symmetric algorithm.

10. (Canceled)

11. (Canceled)

12. (Currently Amended) A method as claimed in claim 1[[1]], in which the portable security module corresponds to one of a smart card and a conditional access module.

13. (Currently Amended) A method as claimed in ~~any of~~ claim[[s]] 1 ~~to 9~~, in which the first decoder ~~device~~ corresponds to a conditional access module and the ~~second device~~ portable security module corresponds to a smart card.

14. (Currently Amended) A method as claimed in ~~any of~~ claim[[s]] 10 ~~to 13~~, in which data encrypted and decrypted with a session key corresponds to control word data.

15. (Currently Amended) A method as claimed in ~~any of~~ claim[[s]] 10 ~~to 13~~, in which data encrypted and decrypted with a session key corresponds to descrambled broadcast data.

16. (Canceled)

17. (Currently Amended) A method as claimed in ~~any of~~ claim[[s]] 1 ~~to 9~~ as applied to a home network system, wherein the first decoder and the portable security module ~~the first and second devices~~ correspond~~ing~~ to ~~first and second~~ consumer electronic devices adapted to transfer data via a communication link.

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Currently Amended) A digital television system for providing secure communication of

data between a first decoder and a portable security module~~second devices~~, said first decoder ~~device~~ comprising a memory for storing at least one precalculated key pair comprising a session key and an encrypted version of the session key prepared using a transport key, and communication means for communicating the encrypted version of the session key to said portable security module ~~second device~~, said portable security module ~~second device~~ comprising a memory for storing an equivalent transport key, decryption means for decrypting said encrypted version of the session key using said equivalent transport key, and means for encrypting data to be communicated to said first decoder ~~device~~ using said session key.

22. (Currently Amended) A system as claimed in claim 21, wherein the memory of the first decoder ~~device~~ is adapted to store a plurality of key pairs, the first decoder ~~device~~ comprising means for selecting and processing at least one session key to generate a definitive session key said communication means being adapted to communicate the associated encrypted version of said at least one session key to the portable security module ~~second device~~, said portable security module ~~second device~~ comprising means for processing said at least one session key to generate the definitive session key.

23. (Currently Amended) A system as claimed in claim 21 ~~or 22~~, in which the encrypted version of a session key includes a signature value readable by the portable security module ~~second device~~ to verify the authenticity of the encrypted version of the session key.

24. (Currently Amended) A system as claimed in ~~any of~~ claim[[s]] 21 ~~to 23~~, in which an algorithm and transport key used to encrypt and decrypt a session key correspond to a symmetric algorithm and associated symmetric key.

25. (Currently Amended) A system as claimed in ~~any of~~ claim[[s]] 21 ~~to 24~~, in which an encryption algorithm used with a session key to encrypt and decrypt data communicated between the first decoder and the portable security module ~~second device~~ corresponds to a symmetric algorithm.

26. (Canceled)

27. (Canceled)

28. (Currently Amended) A system as claimed in claim [[27]] 21, in which the portable security module corresponds to one of a smart card and a conditional access module.

29. (Canceled)

30. (Canceled)

31. (Currently Amended) A system as claimed in ~~any of~~ claim[[s]] 21 ~~to 25~~ as applied to a home network system, wherein the first decoder and the portable security module ~~the first and second devices~~ correspond~~ing~~ to ~~first and second~~ consumer electronic devices adapted to transfer data via a communication link.

32. - 33. (Canceled)